**Azure POC Prep Worksheet**

In Prep for the upcoming work we’re going to do on WVD, please review the following:

The following table contains all the information we will need to interactively cut and paste while using WVD; **since a good deal of this is sensitive information, recommend your team put this information in a secure location that is readily-accessible during the POC.**

The steps to gather all this information are below:

|  |  |  |
| --- | --- | --- |
| **Name** | **Value** | **Notes & How to find** |
| Azure AD Tenant GUID | GUID: | * We need the AAD Tenant GUID identifier so WVD knows which AAD it is querying.   + To do this, open <https://www.whatismytenantid.com/> & plug in the FQDN of your AAD environment - this site will spit out your GUID. |
| Azure Subscription GUID | GUID: | * + Your VMs will be spun up in an Azure Subscription; WVD implementation team must have Contributor rights or above for the Subscription.     - Is the Subscription a Dev / Test Subscription? Has impacts on available VM types & scale.   + Step-by-step: <https://blogs.msdn.microsoft.com/mschray/2016/03/18/getting-your-azure-subscription-guid-new-portal/> |
| User account/Service account that can join VMs to the domain | Username (UPN):  Password: | * + The account MUST NOT use MFA of any sort and requires a complex password of at least 12 characters.   + If you have to create an account just for this purpose that meets these requirements, please do. See: [https://richardstk.com/2013/11/29/create-a-dedicated-account-to-join-computers-to-a-domain/](https://nam06.safelinks.protection.outlook.com/?url=https%3A%2F%2Frichardstk.com%2F2013%2F11%2F29%2Fcreate-a-dedicated-account-to-join-computers-to-a-domain%2F&data=02%7C01%7Cmgarriga%40microsoft.com%7Cb21763a3e873404b4f8408d79a9f21f7%7C72f988bf86f141af91ab2d7cd011db47%7C1%7C0%7C637147880567380129&sdata=8xLCK5rwvvvecL7VMfzDxCxV3GPxsMXuvHlx1L9fyUE%3D&reserved=0)   + DO NOT SHARE this info w/me and/or have it onscreen during our work; these are HIGHLY sensitive creds that are germane to your org.   + We ask that this account pre-created just in case your org has to go through Change Control and/or exceptions to policy based on the above (no MFA) |
| AD OU distinguishedName | OU for VMs supporting desktops:  OU for VMs supporting apps: | * + VMs we spin up will need to be placed in OU containers; please have target OUs selected & pre-built, along with any delegation of management for said OUs.   + We’ll need the distinguishedName of the OU per [https://support.xink.io/support/solutions/articles/1000246165-how-to-find-the-distinguishedname-of-an-ou-](https://nam06.safelinks.protection.outlook.com/?url=https%3A%2F%2Fsupport.xink.io%2Fsupport%2Fsolutions%2Farticles%2F1000246165-how-to-find-the-distinguishedname-of-an-ou-&data=02%7C01%7Cmgarriga%40microsoft.com%7Cb21763a3e873404b4f8408d79a9f21f7%7C72f988bf86f141af91ab2d7cd011db47%7C1%7C0%7C637147880567390122&sdata=buhkWBZF9T7%2BN50Fb%2BkSJnXJPEDcQhB1sCVPHwAnWBQ%3D&reserved=0)     - A distinguishedName looks like this: ***OU=Users,OU=Company\_1OU,DC=Company\_1,DC=internal*** |
| Service Principal Info | $svcPrincipalCreds.Value:  $aadContext.TenantId.Guid:  $svcPrincipal.AppId: | * + Follow the steps here to get the values shown: [https://docs.microsoft.com/en-us/azure/virtual-desktop/create-service-principal-role-powershell](https://nam06.safelinks.protection.outlook.com/?url=https%3A%2F%2Fdocs.microsoft.com%2Fen-us%2Fazure%2Fvirtual-desktop%2Fcreate-service-principal-role-powershell&data=02%7C01%7Cmgarriga%40microsoft.com%7Cb21763a3e873404b4f8408d79a9f21f7%7C72f988bf86f141af91ab2d7cd011db47%7C1%7C0%7C637147880567420112&sdata=ltktp%2BzojGCjFWXGGQlxsNU1eEGPvpBFZ2gxg0UMvj0%3D&reserved=0)   + DO NOT SHARE this info w/me and/or have it onscreen during our work; these are HIGHLY sensitive creds that are germane to your org. |
| Azure Resource Groups for WVD Objects | * + One to place the File Server mentioned below into:   + A Second to place the Desktop VMs in:   + A Third to place the RemoteApp VMs in: | * + Steps to create Resource Groups: <https://docs.microsoft.com/en-us/azure/azure-resource-manager/management/manage-resource-groups-portal#create-resource-groups>   + We ask that these be pre-created just in case they have to go through Change Control and/or require Tags, etc. - helps us avoid errors during deployment   + Placing these objects in Resource Groups make tear-down of a PoC environment geometrically easier |

**Preparation for the Event (POC or Workshop):**

* Validate the major Requirements (reference here: <https://docs.microsoft.com/en-us/azure/virtual-desktop/overview>):
  + Licensing: Microsoft A3, A5 for all users of WVD
  + An Azure Subscription with Contributor rights or above
  + Connectivity between on-premises and Azure via one of the following:
    - Site-to-Site VPN
    - ExpressRoute
  + An on-prem Windows Server AD in sync with AAD, set up with working Azure AD Connect
  + An Azure Active Directory sync’d with your on-premises AD
  + A Virtual Network in the Azure subscription that contains (or is networked to on-prem versions of):
    - AD servers
    - DNS servers
    - Licensing Servers for 3rd party apps
    - **GatewaySubnet** of /28 minimal (higher IP range preferred)
  + Network access to on-premises resources; networking routing in place, network filtering adjusted to allow:
    - AD replication between on-prem AD and Azure-based AD systems
    - DNS name resolution
    - Access to on-prem file servers
    - Access to on-prem printers
* **GPO head’s up:**
  + **Existing GPOs that point to existing KMS servers on-prem (or any other way applied) will cripple your WVD environment; see:** [**https://docs.microsoft.com/en-us/azure/virtual-machines/troubleshooting/custom-routes-enable-kms-activation**](https://docs.microsoft.com/en-us/azure/virtual-machines/troubleshooting/custom-routes-enable-kms-activation)
  + **Shut off GPO-enforced all logon banners – they cause issues**
* We need an Azure AD Global Admin to do 3 things (I’m glad to chat about these steps in detail, either prior to the event or day of… if this is day of the event, best to have your AAD Global Admin in the room w/us):
  + Grant WVD the right to read AAD so users can login (see [https://docs.microsoft.com/en-us/azure/virtual-desktop/overview](https://nam06.safelinks.protection.outlook.com/?url=https%3A%2F%2Fdocs.microsoft.com%2Fen-us%2Fazure%2Fvirtual-desktop%2Foverview&data=02%7C01%7Cmgarriga%40microsoft.com%7Cb21763a3e873404b4f8408d79a9f21f7%7C72f988bf86f141af91ab2d7cd011db47%7C1%7C0%7C637147880567410114&sdata=Gcd8KdvbR7WNzH3QXpoWE2PKsxDKXNtOrUSs8rcmnqQ%3D&reserved=0) the section labeled “Allow the Windows Virtual Desktop service to access Azure AD”)
  + Create a Service Principal for building Host Pools - they will need to hand over the creds for this Service Principal prior to the event - see above table for the values we need & how to get them.
  + Grant other administrators participating in the WVD POC the “WVD Tenant Creator” Role (see [https://docs.microsoft.com/en-us/azure/virtual-desktop/overview](https://nam06.safelinks.protection.outlook.com/?url=https%3A%2F%2Fdocs.microsoft.com%2Fen-us%2Fazure%2Fvirtual-desktop%2Foverview&data=02%7C01%7Cmgarriga%40microsoft.com%7Cb21763a3e873404b4f8408d79a9f21f7%7C72f988bf86f141af91ab2d7cd011db47%7C1%7C0%7C637147880567420112&sdata=TmcsqbkWUsG0PlQqzRjL9vB6qmWlxGb1F0bQZM%2BxjmU%3D&reserved=0) the section labeled “Assign the “TenantCreator” role to a user account”)
* Ensure you have Contributor or above (Owner) role(s) assigned to folks building VMs in the Subscription we’ll use for WVD (repeat of info from above, reinforcing the point that we need this).
* Create three Resource Groups in advance, per the above table ("Azure Resource Groups for WVD Objects")
* Have a designated Azure VNet & Subnet ready to go for placement of the WVD VMs
  + Ensure the above VNet is pointing at existing DNS Servers either on-prem or in Azure (reinforcing this point)
  + Ensure no overlapping IP addresses for on-prem or other cloud providers for the VNet(s) in question
  + Ensure we have control over network port filters and/or other organizational firewall config (or have those folks on speed dial)
  + Steps to ensure your DNS is set properly: <https://docs.microsoft.com/en-us/azure/virtual-network/manage-virtual-network#change-dns-servers>
* Have your AD team create a new Site in Active Directory Sites & Services
  + This step is required when a client has DCs that reside in Azure
  + In setting this up, assign the correct subnets to the Azure-based Site
  + Reference: <https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc772304(v=ws.11)?redirectedfrom=MSDN>
* Have your AD team designate OUs for placement of the WVD VMs
  + Get the DN for each per the table above
  + Have AD team Block GPO Inheritance for these OUs – we do not want existing GPO’s hindering POC work
  + Ensure the account for domain joins (see table above) has rights to created OUs to add machine accounts
* We’ll need a File Server in Azure for hosting FSLogix Profiles & for hosting Software we'll deploy – follow the steps here: <https://docs.microsoft.com/en-us/azure/virtual-machines/windows/quick-create-portal> Specs and key points here:
  + Size/type: **D4s\_v3**
  + Place the VM on the same VNet and Subnet where the WVD VMs will be placed (VERY IMPORTANT)
  + Add a 2nd disk to the VM 1TB or larger (1TB is good enough): <https://docs.microsoft.com/en-us/azure/virtual-machines/windows/attach-managed-disk-portal>
  + Domain-join the File Server VM with these specific instructions:
    - Domain join it using fqdn of your domain (e.g., ***myonpremad.myorg.edu***); this validates that the DNS has been set properly for the VNet.
    - Use the credentials above for joining domain ("User account/Service account that can join VMs to the domain") to ensure those creds work.
  + Create Shares:
    - Create a share called "WVDProfiles" and set permissions on it per: [https://docs.microsoft.com/en-us/azure/virtual-desktop/create-host-pools-user-profile](https://nam06.safelinks.protection.outlook.com/?url=https%3A%2F%2Fdocs.microsoft.com%2Fen-us%2Fazure%2Fvirtual-desktop%2Fcreate-host-pools-user-profile&data=02%7C01%7Cmgarriga%40microsoft.com%7Cb21763a3e873404b4f8408d79a9f21f7%7C72f988bf86f141af91ab2d7cd011db47%7C1%7C0%7C637147880567390122&sdata=6E9fg2UxZLLmnqYhZJm0jbVf8wMFLaGTwIThhjviuzM%3D&reserved=0)
    - Create a Share on the 2nd disk called "Software" and download these binaries to that share in advance of our work in Azure:
      * Any software you want to test during App or Desktop publishing experience.
      * The full RDS client: <https://go.microsoft.com/fwlink/?linkid=2098960>
      * FSLogix software from here: [https://docs.microsoft.com/en-us/fslogix/install-ht](https://nam06.safelinks.protection.outlook.com/?url=https%3A%2F%2Fdocs.microsoft.com%2Fen-us%2Ffslogix%2Finstall-ht&data=02%7C01%7Cmgarriga%40microsoft.com%7Cb21763a3e873404b4f8408d79a9f21f7%7C72f988bf86f141af91ab2d7cd011db47%7C1%7C0%7C637147880567400120&sdata=EMCDVSB9NTi9Ba9EzkaT6zqTiLWNOB%2BaTls8QxehSKg%3D&reserved=0)
        + Prior to the event, copy the ADMX and ADML files from the FSLogix download into your Active Directory environment: [https://docs.microsoft.com/en-us/fslogix/use-group-policy-templates-ht](https://nam06.safelinks.protection.outlook.com/?url=https%3A%2F%2Fdocs.microsoft.com%2Fen-us%2Ffslogix%2Fuse-group-policy-templates-ht&data=02%7C01%7Cmgarriga%40microsoft.com%7Cb21763a3e873404b4f8408d79a9f21f7%7C72f988bf86f141af91ab2d7cd011db47%7C1%7C0%7C637147880567410114&sdata=tkl2Ge%2FzGgUAW3FObETEV0kkEfz9IWLyLvhV9wooiVI%3D&reserved=0)
        + Most orgs require Change Control processes to do this step; if that's tough we can skip ADMX/ADML insertion into AD and just manually create the required Registry Entries.
* Please build/set aside 4-6 User accounts to test with. We’ll assign apps and VMs to these accounts exclusively, so we can work through the Admin experience and then see the separate client experience using different credentials.
  + These users must be in your existing AD and then synced to Azure AD so they are represented in both places using the same UPN in AD/AAD.

Things you need to know/good background info:

* All the VMs we build will join your Active Directory Domain. Accordingly, there should be no hindrance for the above account to join VMs to the Domain (for example: at one client, Domain Join failed unless one had pre-provisioned the AD account for the VM because that’s their required way of joining VMs to the Domain)
  + This implies that your site-to-site link via VPN or ExpressRoute is up and running. We will need this completed prior to the PoC.
* For the VMs we spin up, we will want Admin rights at the OS level; recommend we have a Domain Admin in the room or available via speed dial.
* All the work we do in WVD will be from Windows machines w/PowerShell– PowerShell on Mac/Linux cannot be used to manage WVD.
  + Further, individuals managing WVD will need rights on their local machines to add WVD binaries to PowerShell.
  + VS Code cannot be used w/WVD, either; we'll exclusively be using the PowerShell ISE on Windows machines.
* It’s best if we have GPO manipulation capabilities.
  + We will need to deploy GPOs for FSLogix and we might we run into a GPO blocker that requires remediation (every client’s GPOs can cause issues for a variety of reasons).
  + For example, your institution might have a GPO that shuts off a service or port we need. Would be good to fix that on the fly and/or have those folks on Speed Dial.
  + See [https://docs.microsoft.com/en-us/azure/virtual-desktop/overview](https://nam06.safelinks.protection.outlook.com/?url=https%3A%2F%2Fdocs.microsoft.com%2Fen-us%2Fazure%2Fvirtual-desktop%2Foverview&data=02%7C01%7Cmgarriga%40microsoft.com%7Cb21763a3e873404b4f8408d79a9f21f7%7C72f988bf86f141af91ab2d7cd011db47%7C1%7C0%7C637147880567430106&sdata=XG8lkICBLhANjAlPaBxme0AUf7BT65ae3xftX17HQio%3D&reserved=0) for a list of URLs we need to be able to access over 443 AND 1688 – if you have a “filtering app” resident on the VM to allow/deny internet traffic, this must be modified to support:

| **Address** | **Outbound port** | **Purpose** |
| --- | --- | --- |
| \*.wvd.microsoft.com | TCP port 443 | Service traffic |
| \*.blob.core.windows.net | TCP port 443 | Agent, SXS stack updates, and Agent traffic |
| \*.core.windows.net | TCP port 443 | Agent traffic |
| \*.servicebus.windows.net | TCP port 443 | Agent traffic |
| prod.warmpath.msftcloudes.com | TCP port 443 | Agent traffic |
| catalogartifact.azureedge.net | TCP port 443 | Azure Marketplace |
| kms.core.windows.net | TCP port 1688 | Windows 10 activation |

* Along with the above, it’s best if we have the ability to manipulate the host-based Firewall on the VMs in question, just in case there are exclude rules hindering communications.
* Check Subscription Core Counts – ensure both Regional and VM types have headroom so we can build VMs without running over your quotas:
  + <https://docs.microsoft.com/en-us/azure/azure-resource-manager/templates/error-resource-quota>

|  |  |  |
| --- | --- | --- |
| **Role/Title/Skill** | **Purpose** | **Sub-unit Tasks** |
| **Client Azure AD Team** | Responsible for AAD manipulation and config for WVD environment | * + Validate authorization approach for AAD (e.g., using password hashes, ADFS, etc.)   + Authorize WVD PaaS layer for AAD read access   + Assign WVD Tenant Creators Role   + Create Service Principal for WVD deployments   + Create Azure AD Groups for targeted publishing of Apps and Desktops via scripting |
| **Client WVD Team** | Overall ownership of WVD solution deployment | * + Build WVD Tenant(s) based on org requirements   + Establish Naming Conventions for WVD Hosts, HostPools, Tenant, etc.   + Assign RBAC within WVD Tenant(s)   + Publish App and Desktop HostPools to meet requirements   + Assign HostPools to end users (and AAD Groups via interim scripting solution)   + Validate approach to match Use Cases to deployment plans |
| **Client Networking Team** | Responsible for networking implementation &configuration | * + Establish IP scopes for utilization in Azure   + Build and/or set constraints on Azure-based VNets based on requirements   + Implement site-to-site networking technology to access on-prem resources (licensing servers, legacy systems, etc.) |
| **Client AD Team** | Responsible for AD-level work to support Azure environment running WVD systems | * + Set up Active Directory Sites & Services for new AD site in Azure (need IP Ranges info from Network team)   + Establish DC's in Azure to implement GPOs at LAN Speed   + Validate replication topology is working nominally   + Confirm naming convention for VMs joining Active Directory   + Confirm OU structure for supporting multiple HostPool deployments |
| **Client GPO Team** | Responsible for GPO deployment/analysis/revision throughout the WVD build, test, and deployment | * + Implement GPO's germane to FSLogix   + Analyze existing GPO structure to spot pre-existing GPOs that will have issues in WVD environment   + Build and apply other GPOs to ensure consistent WVD environment (e.g. Time Zones, org wallpaper, common desktop icons, mapped drives, etc.)   + Build and apply GPOs for Session Host Limits (Idle & Disconnected Sessions) |
| **Client Azure Team** | Responsible for overall dissemination of Azure services for all Org implementations, not just WVD | * + Build Azure Subscriptions for Hub and Spoke model   + Apply Azure RBAC based on organizational requirements |
| **Client User Experience / Management team** | Responsible for end-user computing environment (Desktop or Apps) meeting consistent org goals for look & feel | * + Establish Use Cases for remote user pool and prioritize publishing requirements   + Prioritize apps for publication to end-users   + Ensure management and monitoring tools required by the org are on key apps list   + Where needed, manage desktop experience (wallpaper, etc.) and recommend GPO changes to meet expectations |
| **Client CISO Team** | Responsible for establishing Auditing requirements to meet Org security requirements (across Networking, Client config, etc.) | * + Establish baseline security requirements and publish list of what will be audited and how   + Review Networking and RBAC plans from other teams to ensure compliance with existing policies   + Specify which client-centric Data Security requirements must be met in Azure (e.g. HIPAA or other data classifications)   + Validate approach for MFA and tools required for enabling in Azure |
| **Client Server Team / Storage Team** | FSLogix Solution Build | * + Deploy Netapp or File Server shares for FSLogix Profiles |